AMENDMENTS TO THE CLAIMS

1. (Currently amended) A security module, ~~characterized in that it has~~ comprising:

a data input port via which information ~~can be~~ is input into the security module; ~~, in that the security module has at least two data output ports, whereby data can be output via a first data output port and then transferred to an authentication unit and whereby data can be output via a second data output port and then be transferred to a document to be issued, with at least two combination machines (K1, K2), whereby~~

a first combination machine ~~(K1) generates~~ including first means for generating and transferring a first result value ~~for the~~ via a first data output port to an authentication unit; and ~~whereby~~

a second combination machine ~~(K2) generates~~ including second means for generating and transferring a second result value ~~for the~~ via a second data output port to a document to be issued,

wherein the second result value is independent of any information in the document to be issued.

2. (Currently amended) The security module according to Claim 1, ~~characterized in that it has~~ further comprising a secret generator that generates an unpredictable secret.

3. (Currently amended) The security module according to Claim 2, ~~characterized in that~~ wherein the secret generator is connected to at least one of the first combination machine ~~and/or to~~ and the second combination machine in such a way that ~~a~~ the unpredictable secret generated by the secret generator is introduced into one or more of the first combination machine ~~(K1) and/or into~~ and the second combination machine ~~(K2)~~.

4. (Currently amended) The security module according to ~~one or more of the~~

~~preceding claims, characterized in that it has~~ claim 1, further comprising an identification register, ~~whereby~~

wherein an output value of the identification register is ~~connected~~ provided to the first combination machine ~~(K1)~~ in such a manner that a value of the identification register is introduced into a data combination issued by the first combination machine.

5. (Currently amended) The security module according to ~~one or more of the preceding claims, characterized in that it has~~ claim 1, further comprising at least one encryption machine that encrypts an output value of one of the first and second combination machines ~~(K1)~~.

6. (Currently amended) The security module according to Claim 5, ~~characterized in that the encryption machine is connected to~~ further comprising a key register coupled to the at least one encryption machine, ~~whereby~~ wherein at least one value contained in the key register ~~can be~~ is used ~~in~~ by the encryption machine for encryption purposes.

7. (Currently amended) The security module according to ~~one or more of the preceding claims, characterized in that it has~~ claim 1, further comprising a hash machine.

8. (Currently amended) A method for producing a forgery-proof ~~documents~~document to be issued, ~~whereby input data is input~~ the method comprising:

entering input data into ~~a data~~ an input port of a security module ~~and whereby the security module generates~~ ;

generating information in the security module ~~that serves~~ to identify ~~individual documents, characterized in that~~ an individual document;

combining the input data is ~~input into a data input port of a security module, where it is combined~~ with data representing a secret; ~~and in that~~

further processing the secret ~~is further processed in a processing step~~ separate from the

combining ~~operation, and in that~~ step; and

acquiring data ~~is acquired~~ from the combination of ~~the~~ data representing the secret and the input data,

wherein the combination of data representing the secret and the input data is determined independently from contents of the individual document.

9. (Currently amended) The method according to Claim 8, ~~characterized in that the~~ further comprising:

outputting the further processed secret ~~is output by~~ via a first data output port; and ~~in that the~~

outputting data acquired from the combination of ~~the~~ data representing the secret and the input data ~~is output~~ at a second data output port.

10. (Currently amended) The method ~~according to one or more of the preceding claims, characterized in that the~~ of claim 8, further comprising combining data representing the secret and the input data ~~are combined in a second combination machine (K2)~~.

11. (Currently amended) The method according to Claim 10, ~~characterized in that the~~ further comprising irreversibly linking data representing the secret and the input data ~~are irreversibly linked~~ to each other, ~~whereby this irreversible~~

wherein said step of irreversibly linking is done in such a way that, exclusively when the same data is linked again in ~~the~~ a same manner, an identical result is obtained, without allowing any conclusions about the ~~temporary~~ secret.

12. (Currently amended) The method ~~according to one or more of Claims 8 through 11, characterized in that~~ of claim 8, further comprising linking the data representing the secret ~~is further linked~~ while introducing data of an identification register.

13. (Currently amended) The method according to Claim 12, ~~characterized in that the~~ further comprising encrypting a result of ~~the~~ a combination of the data representing the secret and ~~the~~ data of the identification register ~~(ID) is encrypted in an encryption machine~~.

14. (Currently amended) The method according to Claim 13, ~~characterized in that the encryption takes place while~~ further comprising, simultaneously carrying out said encrypting while introducing a key whose value is stored in a key register ~~(SR)~~.

15. (Currently amended) The method ~~according to one of more of Claims 8 through 14, characterized in that this~~ of claim 9, further comprising transferring data that is output from the first data output port ~~is transferred~~ to an authentication unit.

16. (Currently amended) The method according to Claim 15, ~~characterized in that the~~ further comprising linking, through the authentication unit, ~~links~~ the transferred data with another key.

17. (Currently amended) The method ~~according to one of more of Claims 8 through 16, characterized in that~~ of claim 9 wherein said step of outputting data at ~~the data that is output from~~ the second data output port ~~is output as~~ comprises outputting forgery-proof information to the forgery-proof documents to be issued.

18. (New) The security module of claim 1, wherein the first means for generating processes an unpredictable secret from a secret generator and an output value from an identification register.

19. (New) The security module of claim 1, wherein the second means for generating processes an unpredictable secret from a secret generator and information input via the data input port.

20. (New) A security module for producing a forgery-proof document, the module comprising:

an identification register, a key register and a secret generator that generates an unpredictable secret;

a first combination machine that combines an output of the identification register and an output of the secret generator;

an encryption machine that encrypts an output of the first combination machine;

a first outlet valve that outputs an encrypted output of the encryption machine via an authentication unit;

a second combination machine that combines the unpredictable secret and input data received via an inlet valve;

a hash machine that generates an irreversible hash value responsive to an output of the second combination machine; and

a second outlet valve that outputs the hash value,

wherein the hash value is independent of contents of the forgery proof document.

21. (New) The security module of claim 20, further comprising a key register coupled to the encryption machine, wherein at least one value stored in the key register is used by the encryption machine to provide the encrypted output of the first combination machine.

22. (New) A method for producing a forgery-proof document, the method comprising:

using the security module of claim 18; and

outputting the hash value from the second outlet valve as forgery-proof information to the forgery-proof document.

23. (New) A method for producing a forgery-proof document, the method comprising:

generating an unpredictable secret;

combining an output of an identification register and the unpredictable secret;

encrypting the combined output of the identification register and the unpredictable secret;

outputting the encrypted combined output to an authentication unit;

combining the secret and the input data input via an inlet valve;

using the combined secret and input data to form an irreversible hash value; and

outputting the hash value,

wherein the hash value is independent of contents of the forgery proof document.

24. (New) The method of claim 23, wherein said outputting comprises outputting the hash value to the forgery-proof document.

25. (New) A security module useful for generating a digital franking mark, the module comprising:

means for inputting information into the security module;

a secret generator that generates an unpredictable secret;

means for combining the unpredictable secret and the input information and producing combined data;

hash generating means responsive to the combined data for generating and transferring

the digital franking mark to a letter to be mailed,

wherein the generated digital franking mark is independent of contents of the letter to be mailed.

26. (New) A security module suitable for communicating with an authentication unit, the module comprising:

a secret generator that generates an unpredictable secret;

means for combining an output of an identification register and the unpredictable secret;

an encryption machine that provides an encrypted output responsive at least to the combined output of the identification register and the unpredictable secret; and

means for outputting the encrypted output to the authentication unit.

27. (New) The security module of claim 26, further comprising a key register, wherein a value contained in the key register is provided to the encryption machine and used therein to provide the encrypted output.